

# PATENT COOPERATION TREATY

PCT

## NOTIFICATION OF ELECTION (PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Assistant Commissioner for Patents  
United States Patent and Trademark  
Office  
Box PCT  
Washington, D.C. 20231  
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing: 08 June 2000 (08.06.00)	
International application No.: PCT/EP99/08157	Applicant's or agent's file reference: 402552WO
International filing date: 25 October 1999 (25.10.99)	Priority date: 02 December 1998 (02.12.98)
Applicant: KERKDIJK, Hendrikus	

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International preliminary Examining Authority on:  
08 February 2000 (08.02.00)

☐ in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was  
☐ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	Authorized officer:  J. Zahra Telephone No.: (41-22) 338.83.38
-----------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION  
International Bureau



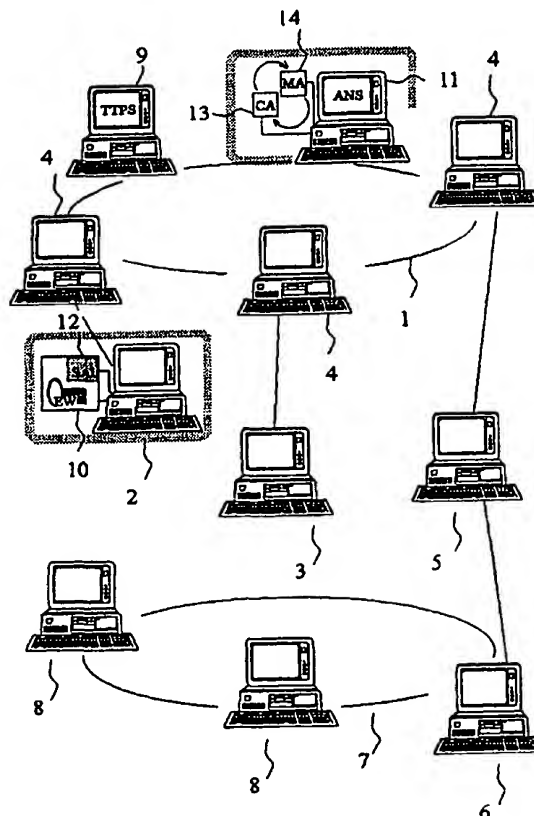
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<b>(51) International Patent Classification <sup>7</sup> :</b> <b>G06F 17/60, G07F 7/10</b>	<b>A1</b>	<b>(11) International Publication Number:</b> <b>WO 00/33219</b> <b>(43) International Publication Date:</b> 8 June 2000 (08.06.00)
<b>(21) International Application Number:</b> PCT/EP99/08157 <b>(22) International Filing Date:</b> 25 October 1999 (25.10.99) <b>(30) Priority Data:</b> 98204063.6 2 December 1998 (02.12.98) EP <b>(71) Applicant (for all designated States except US):</b> KONINKLIJKE KPN N.V. [NL/NL]; Stationsplein 7, NL-9726 AE Groningen (NL). <b>(72) Inventor; and</b> <b>(75) Inventor/Applicant (for US only):</b> KERKDIJK, Hendrikus [NL/NL]; Oostersingel 23/19, NL-9713 EX Groningen (NL). <b>(74) Agent:</b> KLEIN, Bart; Koninklijke KPN N.V., P.O. Box 95321, NL-2509 CH The Hague (NL).		<b>(81) Designated States:</b> AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).  <b>Published</b> With international search report.

**(54) Title:** SYSTEM FOR SECURE TRANSACTIONS

**(57) Abstract**

A multimedia network (1) with connected customer stations (2), merchant servers (3), and a payment server (5). Secure electronic transactions are performed using a secure electronic transactions protocol (SET), including exchange of digital certificates, managed by a Trusted Third Party Server (9). The customer stations comprise transactions management means (10), fit for performing said SET protocol and for managing said certificates for the customer station. A remote customer agent (13) represents the customer station in the negotiation and payment process. The customer station (2) comprises an agent interface (12), fit for transmission of codes, parameters and certificates between the customer agent (13) and the transactions management means (10). A remote merchant agent (14) represents the merchant station (3) in the negotiation and payment process with the customer agent (13) or the customer station (3), to have paid for the selected products in a secure way, under control of SET protocol.



**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

## System for secure transactions

## BACKGROUND OF THE INVENTION

The invention relates to a system for the execution of  
5 secure transactions in a multimedia network.  
Multimedia networks like the Internet offer a wide variety  
of new possibilities, which will have a great impact on the  
business environment of the future. Various vendors will  
10 start to exploit the Internet as a marketplace. For a  
customer not to get lost within the vast amount of  
information that is provided, in the near future agent-  
based services shall be implemented. Agents are autonomous  
pieces of software, which may perform tasks for users on  
the Internet. Based on the user's preferences, they may  
15 assist the user in making a selection within the vast range  
of offered products. Complementary to this, the agent may  
assist in the actual purchase of such a product. As part of  
this process, the agent will have to be able to perform  
payments.  
20 One of the biggest inhibitors on Electronic Commerce today  
is security. Consumers demand that their private  
information be kept private. When using agent technology  
within an E-Commerce service, adequate security precautions  
must be taken. At present, however, agent security is still  
25 in its infancy. Therefore, delegating payments to agents is  
not possible at this moment in time.

## SUMMARY OF THE INVENTION

According to the present invention, an architecture is  
30 proposed in which agents may perform secure credit card  
payments. According to the invention, for the execution of  
such payments the SET (Secure Electronic Transactions)  
protocol is used, an upcoming standard for secure payments  
on the Internet by means of credit cards. All new entities  
35 and components that are necessary to provide agent-based  
SET payments will be defined and payment interaction  
(agent-agent, agent-user and other) will be elaborated  
upon.

-2-

Most entities of the standard infrastructure for performing SET-based payments by means of credit cards are straightforward analogies to real world credit card payments. A few, however, need further explanation. A brief  
5 description of these will be given first.

One of the main issues when providing secure payments is authentication of the involved entities. SET uses a robust set of digital certificates for this purpose. Each participant in a SET transaction requires a specific  
10 certificate or set of certificates that not only uniquely identifies this participant, but also attests to his or her privilege as holder of a payment card or as a holder of a Merchant account. Brand Associations (e.g. VISA/MasterCard) or Card Issuers commission so called  
15 Certificate Authorities (CAs) to carry out the work of managing SET digital certificates.

Complementary to this, SET introduces the notion of a Payment Gateway, which is needed to validate SET digital certificates and preprocess authorisation, capture and  
20 settlement work concerning the payment at hand. Another fundamental requirement for performing SET payments is a component called an Electronic Wallet (E-Wallet). These wallets embody the SET protocol on the customer side and provide a means to store and manage the certificates to  
25 digitally sign messages, along with the security aspects consumers demand to keep private data private.

According to the present invention the task of performing SET credit card transactions is delegated to agents. In developing an infrastructure that enables this, the  
30 following constraints have been defined:

- Obtaining certificates is not a task that users will want to delegate to their agents. Furthermore, it is not very probable that banks and CAs will approve of this situation. Therefore, we assume all certificates and the E-Wallet to  
35 be in place.
- The standard SET infrastructure shall be kept intact.

-3-

Thereby the inherent security of SET payments shall remain present and the necessary alterations when implementing shall be limited.

Based on these constraints, an infrastructure has been  
5 designed which will be discussed below.

#### EMBODIMENT OF THE INVENTION

Figure 1 shows an architecture in which the invention -the use the SET protocol by "secure agents- can be implemented.  
10 Figure 1 shows a multimedia network -the internet- 1. Connected to the internet 1 are customer PCs 2, and merchant servers 3, each via an internet service providers (ISP) 4. Also connected to the internet, via an ISP 4, is a payment (gateway) server 5. The payment server 5 is also -  
15 via an access server 6- connected to a "Banker's Interchange Network" (BIN) 7, having banking servers 8 connected to it.

A main issue in secure payments is authentication of entities. The SET protocol, to be used in the system shown  
20 in figure 1, uses a set of digital certificates for this purpose. Each participant in transaction requires a certificate that uniquely identifies the participant and also attests to his privilege as a holder of an account at the merchant server. Associations like VISA/MasterCard or  
25 other Card Issuers commission so called Certificate Authorities to carry out the work of managing SET digital certificates. In figure 1 a Trusted Third Party Server (TTPS) 9 of such Certificate Authority is connected to the internet 1 and can be approached by customers 2, merchants  
30 3 and payment servers 5. Payment servers 5 are needed to validate the digital certificates and to preprocess authorisation, capture and settlement work concerning the payment.

Another fundamental requirement for performing SET payments  
35 is a system component called "Electronic Wallet" (EW) 10.

An E-wallet 10 embodies the SET protocol at the customer's side and provides means --within the customer's PC 2-- to store and manage the needed certificates, to digitally sign messages, along with the security aspects customers demand to keep private data private.

According to the invention agents are used to perform secure transactions. As said before, agents are autonomous pieces of software, which are enabled to perform tasks for users (customers or merchants). Based on preferences set by users 2 (customer) and 3 (merchant), the users' respective agents assist or represent the users in presenting and selecting of the merchants' products and, complementary to this, the users' respective agents assist or represents the users to purchase (collect) the selected products and to perform the secure payment for it.

Each customer 2 may be represented by a customer agent (CA), while each merchant 3 may be represented by a merchant agent (MA). The negotiation process (presentation, selection and collection of products and the payments for the collected products) is executed within an "agent platform", preferably embodied within an "Agent Negotiation Server" (ANS) 11. Communication between the customer's PC 3 and the customer's agent at the ANS's side is performed, at the customer's side via the E-wallet 10 --meant for SET based transaction-- which is extended with a special SET Agent Interface (SAI) 12.

The CA 13 communicates with the customer by means of the customer's "browser" (customer interface) and, via the SAI 12, with the customer's E-Wallet 10 in order to initialise payments. As was the case according to the state-of-the-art (using credit cards), the actual SET payment process is performed between the E-Wallet 10 and the Merchant server 3. Therefore, during actual payment interaction the level of trust is the same as in known, credit card based SET payments.

-5-

The CA 13 will have to be authorised to initialise the EW 10 for payments. In standard SET transactions the customer is prompted --via the customer's browser-- to enter the E-Wallet password for this purpose. The CA 13 and the SAI 12  
5 will have to be implemented such, that one of two scenarios may be performed: either the CA 13 has authorisation to release the cryptographic content of the E-Wallet 10 itself, or, after agent initialisation, the customer is prompted to provide an E-Wallet password. In the latter  
10 case, customer interaction is necessary. This is not desirable from a usability point of view, but might be preferred by customers (or merchants), since this will give them a sense of control over the payment.

Figure 2 shows a communication procedure for the system  
15 presented in figure 1.

For authentication and authorisation purposes, the CA 13 will carry a token, in which an authorisation code for opening up the E-Wallet is encapsulated. The level at which this token is secured within the agent depends on the  
20 location of the platform in which the CA 13 performs its tasks. If this platform resides on the customer PC, security requirements on both storing the token within the agent and communicating it to the E-Wallet are less strong than if the agent resides on a remote platform like the ANS  
25 11 as suggested in figure 1. In the latter case, the token will need to be adequately secured, as will. communication between the agent and the E-Wallet. The security requirements are as follows:

The token is stored within the CA 13 in encrypted form,  
30 using a random key. A symmetric encryption scheme, such as DES, shall be applied here. This random key is generated at the PC 2 for each specific purchase. A new key shall be generated for each item that is to be bought by the agent.

35 For communication purposes, both the customer 2 and the CA 13 need to own a specific certificate, other than the



- SET certificate. Payment start messages shall be communicated to the E-Wallet 10 in encrypted form, using a random session key. A symmetric encryption scheme, such as DES, shall be applied here. In turn, this random key shall be sent over in encrypted form, using the customer's public key related to the communication certificate. The message shall be signed with the agent's private key and a time stamp shall be added to the message in order to prevent replay by malicious parties.
- 10 In figure 2 the following communication steps are performed:
- In step I, the CA 13 requests the Merchant Agent (MA) 14 to pay by credit card. The latter then informs the merchant server 3 of the requested payment, while parallel to that the CA 13 initialises the EW 10.
- 15 In step II, the standard SET procedure is performed by the EW 10, the Merchant server 3 and the Payment Gateway server 5.
- 20 Finally, in step III, after completion of the payment, the Merchant server 3 informs the MA 14 of this fact. The MA 14 passes this message on to the CA 13, which notifies the customer of payment completion.
- 25 The infrastructure and message flows are a natural extension of any agent-based infrastructure. Implementation may therefore be performed straightforwardly.

## CLAIMS

1. System for the execution of secure transactions in a multimedia network, comprising a multimedia network with customer stations (2), merchant servers (3), and a payment server (5) connected to it, secure electronic transactions being performed using a secure electronic transactions protocol, comprising the exchange of digital certificates, uniquely identifying the relevant transaction participants and also attesting their privileges at the merchant server, said certificates being managed by a Trusted Third Party Server (9) being connected too to said multimedia network, said payment servers 5 being enabled to validate the digital certificates presented and to process authorisation concerning the payment, said customer stations comprising transactions management means (10), fit for performing said secure electronic transactions protocol and for managing said certificates for the customer station, characterized in a remote customer agent (13), managed by agent parameters received or to be received from said customer station (2) and thus, under the control of said parameters, assisting or representing the customer station in a negotiation process, including selecting products to be presented by the merchant server (3), and payment for selected products in a secure way, under control of said secure electronic transactions protocol and said certificates, being managed by said transactions management means (10).
2. System according to claim 1, characterized in that said customer station (2) comprises an agent interface 12, fit for transmission of codes, parameters and certificates between said customer agent (13) and said transactions management means (10).
3. System according to claim 1, characterized in a remote merchant agent (14), managed by agent parameters received or to be

- received from said merchant station (3) and thus, under the control of said parameters, assisting or representing the merchant station in a negotiation process, including presenting products to the customer agent (13) or the customer station (3), and to have paid for products being selected by the customer agent (13) or the customer station (3), in a secure way, under control of said secure electronic transactions protocol and said certificates.
4. System according to claim 2,  
10 c h a r a c t e r i z e d i n that said negotiation and payment process by said customer agent (13) and said merchant agent (14) is performed within an agent negotiation server (11), connected to said multimedia network (1).
- 15 5. System according to claim 1,  
c h a r a c t e r i z e d i n that, within said secure electronic transaction protocol, for authentication and authorisation said customer agent (13) transmits a token is encapsulated, comprising an authorisation code for opening  
20 up said transactions management means (10).
6. System according to claim 5,  
c h a r a c t e r i z e d i n that said token is stored within the customer agent (13) in an encrypted form, using a random key, being generated at the customer station (2)  
25 for each new payment process.
7. System according to claim 5,  
c h a r a c t e r i z e d i n that both the customer station (2) and the customer agent (13) comprise a specific communication certificate, payment start messages being  
30 communicated to said transactions management means (10) in encrypted form, using a random session key which, in turn, is sent over in encrypted form, using the customer station's public key related to said communication certificate, said message being signed with the customer  
35 agent's private key related to said communication

certificate and a time stamp being added to said message in order to prevent replay by malicious parties.

8. Method for the execution of secure transactions in a multimedia network, comprising a multimedia network with
- 5 customer stations (2), merchant servers (3), and a payment server (5) connected to it, secure electronic transactions being performed using a secure electronic transactions protocol, comprising the exchange of digital certificates, uniquely identifying the relevant transaction participants
- 10 and also attesting their privileges at the merchant server, said certificates being managed by a Trusted Third Party Server (9) being connected too to said multimedia network, said payment servers 5 being enabled to validate the digital certificates presented and to process authorisation
- 15 concerning the payment, said customer stations comprising transactions management means (10), fit for performing said secure electronic transactions protocol and for managing said certificates for the customer station, moreover, comprising a remote customer agent (13), managed by agent
- 20 parameters received or to be received from said customer station (2) and thus, under the control of said parameters, assisting or representing the customer station in a negotiation process, including selecting products to be presented by the merchant server (3), and payment for
- 25 selected products in a secure way, under control of said secure electronic transactions protocol and said certificates, being managed by said transactions management means (10), while, moreover, said customer station (2) comprises an agent interface (12), fit for transmission of
- 30 codes, parameters and certificates between said customer agent (13) and said transactions management means (10), and, besides, a remote merchant agent (14), managed by agent parameters received or to be received from said merchant station (3) and thus, under the control of said
- 35 parameters, assisting or representing the merchant station in a negotiation process, including presenting products to

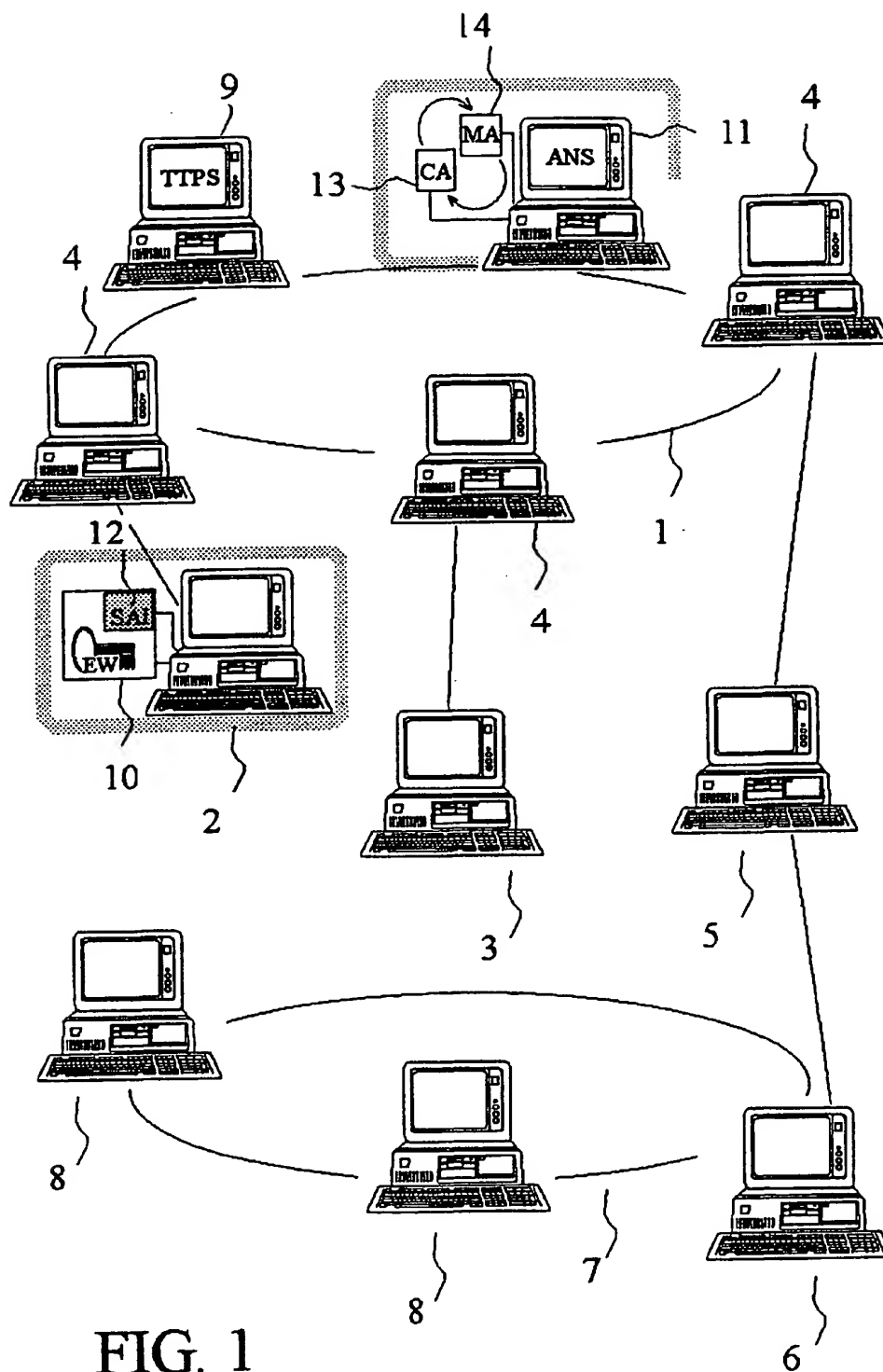
the customer agent (13) or the customer station (3), and to have paid for products being selected by the customer agent (13) or the customer station (3), in a secure way, under control of said secure electronic transactions protocol and  
5 said certificates, characterized in the following communication steps:

in a first step, said customer agent (13) requests said merchant agent (14) to pay by credit card, and the merchant agent then informs said merchant server (3) of the  
10 requested payment, while parallel to that the the customer agent (13) initialises said transactions management means (10);

in a second step, a standard secure electronic transaction procedure is performed by the transactions management means  
15 (10), the merchant server (3) and the payment gateway server (5);

in a third, final step, after completion of the payment process, the merchant server (3) informs the merchant agent (14) of that completion of the payment process, and the  
20 merchant agent (14) passes this message on to the customer agent (13), which notifies the customer station (2) of the payment completion.

1/2



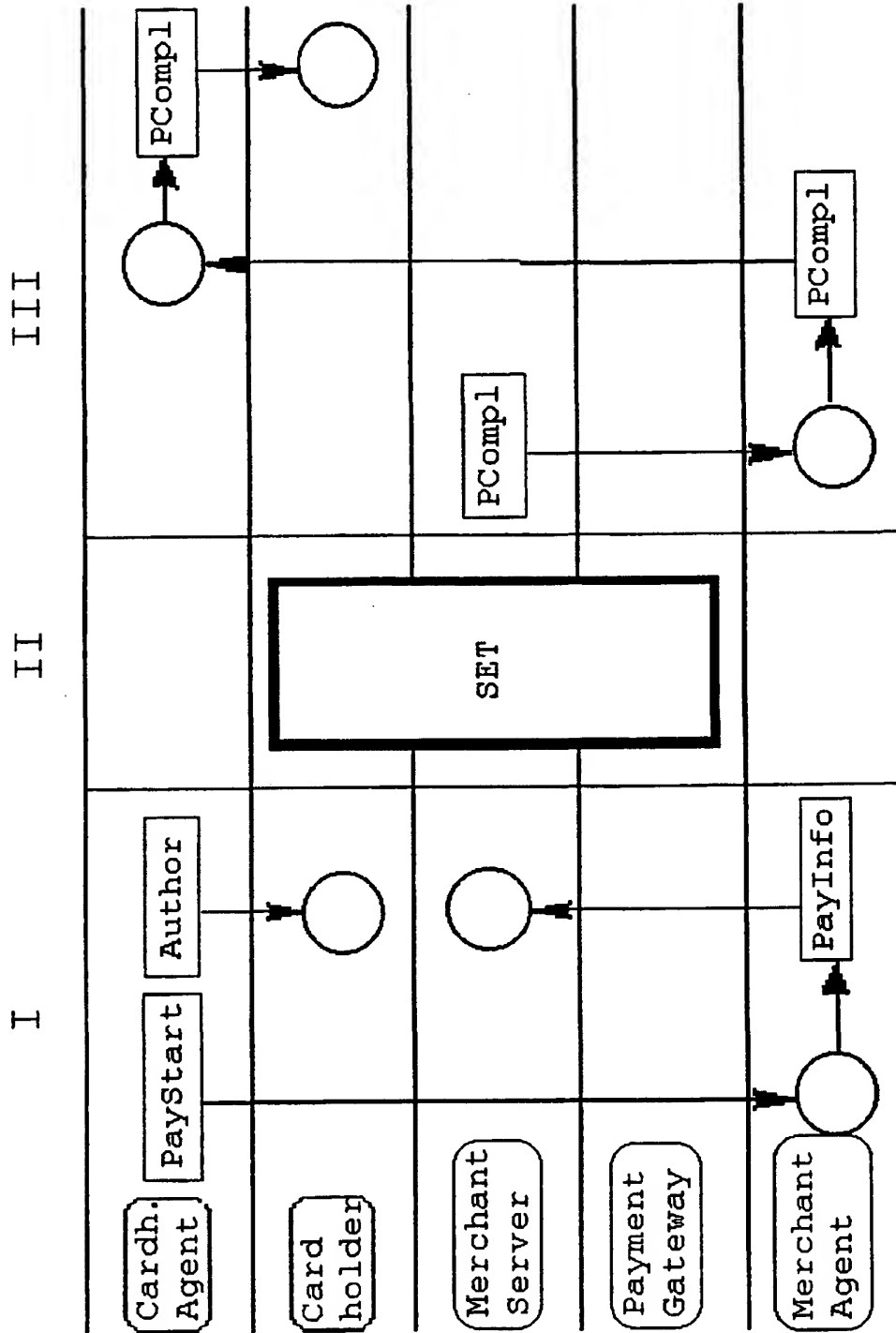


FIG. 2

# INTERNATIONAL SEARCH REPORT

International Application No  
PCT/EP 99/08157

**A. CLASSIFICATION OF SUBJECT MATTER**  
IPC 7 G06F17/60 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)  
IPC 7 G06F G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 671 280 A (ROSEN SHOLOM S) 23 September 1997 (1997-09-23) column 1, line 1 - line 13 column 2, line 15 - line 50 column 5, line 65 -column 6, line 63 column 9, line 46 -column 10, line 64 ----- -/--	1-8

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

\* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

25 January 2000

Date of mailing of the international search report

02/02/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Pedersen, N



# INTERNATIONAL SEARCH REPORT

International Application No  
PCT/EP 99/08157

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>XUN YI ET AL: "A secure auction-like negotiation protocol for agent-based Internet trading"</p> <p>PROCEEDINGS SEVENTEENTH IEEE SYMPOSIUM ON RELIABLE DISTRIBUTED SYSTEMS (CAT. NO.98CB36281), WEST LAFAYETTE, IN, USA, 20 - 23 October 1998, pages 197-203, XP002100668</p> <p>ISBN 0-8186-9218-9, 1998, Los Alamitos, CA, USA, IEEE Comput. Soc, USA</p> <p>page 197, column 2, line 2 - line 6</p> <p>page 198, column 2, line 5 -page 199, column 2, line 41</p> <p style="text-align: center;">---</p>	1-8
A	<p>"SET Secure Electronic Transaction Specification, Book 1: Business Description"</p> <p>31 May 1997 (1997-05-31) , SETCO, MASTERCARD INTERNATIONAL, VISA INTERNATIONAL ,</p> <p>(<a href="http://www.setco.org/download.html">HTTP://WWW.SETCO.ORG/DOWNLOAD.HTML</a>)</p> <p>XP002100669</p> <p>Retrieved from the internet 20th April 1999</p> <p>page 30 -page 72</p> <p style="text-align: center;">---</p>	1-8
A	<p>US 5 790 677 A (SPELMAN JEFFREY F ET AL)</p> <p>4 August 1998 (1998-08-04)</p> <p>column 2, line 6 -column 4, line 39</p> <p style="text-align: center;">---</p>	1-8
A	<p>WO 97 26612 A (PERSONAL AGENTS INC)</p> <p>24 July 1997 (1997-07-24)</p> <p>page 1, line 11 - line 16</p> <p>page 26, line 20 -page 32, line 19</p> <p>figures 1,2</p> <p style="text-align: center;">-----</p>	1-8

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 99/08157

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5671280 A	23-09-1997	AU 699117 B AU 5426496 A CA 2229012 A EP 0886839 A EP 0952562 A HU 9801636 A JP 11500555 T NZ 306096 A PL 325154 A WO 9708665 A	19-11-1998 19-03-1997 06-03-1997 30-12-1998 27-10-1999 28-10-1998 12-01-1999 28-10-1998 06-07-1998 06-03-1997
US 5790677 A	04-08-1998	NONE	
WO 9726612 A	24-07-1997	AU 1836297 A CA 2242874 A EP 0876652 A	11-08-1997 24-07-1997 11-11-1998

System for secure transactions

INSAI

#### BACKGROUND OF THE INVENTION

- The invention relates to a system for the execution of
- 5 secure transactions in a multimedia network.
- Multimedia networks like the Internet offer a wide variety of new possibilities, which will have a great impact on the business environment of the future. Various vendors will start to exploit the Internet as a marketplace. For a
- 10 customer not to get lost within the vast amount of information that is provided, in the near future agent-based services shall be implemented. Agents are autonomous pieces of software, which may perform tasks for users on the Internet. Based on the user's preferences, they may
- 15 assist the user in making a selection within the vast range of offered products. Complementary to this, the agent may assist in the actual purchase of such a product. As part of this process, the agent will have to be able to perform payments.
- 20 One of the biggest inhibitors on Electronic Commerce today is security. Consumers demand that their private information be kept private. When using agent technology within an E-Commerce service, adequate security precautions must be taken. At present, however, agent security is still
- 25 in its infancy. Therefore, delegating payments to agents is not possible at this moment in time.

#### SUMMARY OF THE INVENTION

- According to the present invention, an architecture is
- 30 proposed in which agents may perform secure credit card payments. According to the invention, for the execution of such payments the SET (Secure Electronic Transactions) protocol is used, an upcoming standard for secure payments on the Internet by means of credit cards. All new entities
- 35 and components that are necessary to provide agent-based SET payments will be defined and payment interaction (agent-agent, agent-user and other) will be elaborated upon.

0957383-060101

Most entities of the standard infrastructure for performing SET-based payments by means of credit cards are straightforward analogies to real world credit card payments. A few, however, need further explanation. A brief  
5 description of these will be given first.

One of the main issues when providing secure payments is authentication of the involved entities. SET uses a robust set of digital certificates for this purpose. Each participant in a SET transaction requires a specific  
10 certificate or set of certificates that not only uniquely identifies this participant, but also attests to his or her privilege as holder of a payment card or as a holder of a Merchant account. Brand Associations (e.g. VISA/MasterCard) or Card Issuers commission so called  
15 Certificate Authorities (CAs) to carry out the work of managing SET digital certificates.

Complementary to this, SET introduces the notion of a Payment Gateway, which is needed to validate SET digital certificates and preprocess authorisation, capture and  
20 settlement work concerning the payment at hand. Another fundamental requirement for performing SET payments is a component called an Electronic Wallet (E-Wallet). These wallets embody the SET protocol on the customer side and provide a means to store and manage the certificates to  
25 digitally sign messages, along with the security aspects consumers demand to keep private data private.

According to the present invention the task of performing SET credit card transactions is delegated to agents. In developing an infrastructure that enables this, the  
30 following constraints have been defined:

- Obtaining certificates is not a task that users will want to delegate to their agents. Furthermore, it is not very probable that banks and CAs will approve of this situation. Therefore, we assume all certificates and the E-Wallet to  
35 be in place.
- The standard SET infrastructure shall be kept intact.

0957333-060101  
TOT090-03E75B60

Thereby the inherent security of SET payments shall remain present and the necessary alterations when implementing shall be limited.

Based on these constraints, an infrastructure has been  
5 designed which will be discussed below.

#### EMBODIMENT OF THE INVENTION

Figure 1 shows an architecture in which the invention -the use the SET protocol by "secure agents- can be implemented.  
10 Figure 1 shows a multimedia network -the internet- 1. Connected to the internet 1 are customer PCs 2, and merchant servers 3, each via an internet service providers (ISP) 4. Also connected to the internet, via an ISP 4, is a payment (gateway) server 5. The payment server 5 is also -  
15 via an access server 6- connected to a "Banker's Interchange Network" (BIN) 7, having banking servers 8 connected to it.

A main issue in secure payments is authentication of entities. The SET protocol, to be used in the system shown  
20 in figure 1, uses a set of digital certificates for this purpose. Each participant in transaction requires a certificate that uniquely identifies the participant and also attests to his privilege as a holder of a account at the merchant server. Associations like VISA/MasterCard or  
25 other Card Issuers commission so called Certificate Authorities to carry out the work of managing SET digital certificates. In figure 1 a Trusted Third Party Server (TTPS) 9 of such Certificate Authority is connected to the internet 1 and can be approached by customers 2, merchants  
30 3 and payment servers 5. Payment servers 5 are needed to validate the digital certificates and to preprocess authorisation, capture and settlement work concerning the payment.

Another fundamental requirement for performing SET payments  
35 is a system component called "Electronic Wallet" (EW) 10.

09857383-060101  
T01090-EBE/5860

-4-

An E-wallet 10 embodies the SET protocol at the customer's side and provides means --within the customer's PC 2-- to store and manage the needed certificates, to digitally sign messages, along with the security aspects customers demand to keep private data private.

According to the invention agents are used to perform secure transactions. As said before, agents are autonomous pieces of software, which are enabled to perform tasks for users (customers or merchants). Based on preferences set by users 2 (customer) and 3 (merchant), the users' respective agents assists or represent the users in presenting and selecting of the merchants' products and, complementary to this, the users' respective agents assist or represents the users to purchase (collect) the selected products and to perform the secure payment for it.

Each customer 2 may be represented by a customer agent (CA), while each merchant 3 may be represented by a merchant agent (MA). The negotiation process (presentation, selection and collection of products and the payments for the collected products) is executed within an "agent platform", preferably embodied within an "Agent Negotiation Server" (ANS) 11. Communication between the customer's PC 3 and the customer's agent at the ANS's side is performed, at the customer's side via the E-wallet 10 --meant for SET based transaction-- which is extended with a special SET Agent Interface (SAI) 12.

The CA 13 communicates with the customer by means of the customer's "browser" (customer interface) and, via the SAI 12, with the customer's E-Wallet 10 in order to initialise payments. As was the case according to the state-of-the-art (using credit cards), the actual SET payment process is performed between the E-Wallet 10 and the Merchant server 3. Therefore, during actual payment interaction the level of trust is the same as in known, credit card based SET payments.

09857383-060101

10957383 "060101  
TOT090" E8E258D

The CA 13 will have to be authorised to initialise the EW 10 for payments. In standard SET transactions the customer is prompted --via the customer's browser-- to enter the E-Wallet password for this purpose. The CA 13 and the SAI 12 5 will have to be implemented such, that one of two scenarios may be performed: either the CA 13 has authorisation to release the cryptographic content of the E-Wallet 10 itself, or, after agent initialisation, the customer is prompted to provide an E-Wallet password. In the latter 10 case, customer interaction is necessary. This is not desirable from a usability point of view, but might be preferred by customers (or merchants), since this will give them a sense of control over the payment.

Figure 2 shows a communication procedure for the system 15 presented in figure 1.

For authentication and authorisation purposes, the CA 13 will carry a token, in which an authorisation code for opening up the E-Wallet is encapsulated. The level at which this token is secured within the agent depends on the 20 location of the platform in which the CA 13 performs its tasks. If this platform resides on the customer PC, security requirements on both storing the token within the agent and communicating it to the E-Wallet are less strong than if the agent resides on a remote platform like the ANS 25 11 as suggested in figure 1. In the latter case, the token will need to be adequately secured, as will. communication between the agent and the E-Wallet. The security requirements are as follows:

30 The token is stored within the CA 13 in encrypted form, using a random key. A symmetric encryption scheme, such as DES, shall be applied here. This random key is generated at the PC 2 for each specific purchase. A new key shall be generated for each item that is to be bought by the agent.

35 For communication purposes, both the customer 2 and the CA 13 need to own a specific certificate, other than the

- SET certificate. Payment start messages shall be communicated to the E-Wallet 10 in encrypted form, using a random session key. A symmetric encryption scheme, such as DES, shall be applied here. In turn, this random key shall be sent over in encrypted form, using the customer's public key related to the communication certificate. The message shall be signed with the agent's private key and a time stamp shall be added to the message in order to prevent replay by malicious parties.
- 5
- 10 In figure 2 the following communication steps are performed:

- In step I, the CA 13 requests the Merchant Agent (MA) 14 to pay by credit card. The latter then informs the merchant server 3 of the requested payment, while parallel to that the CA 13 initialises the EW 10.
- 15

In step II, the standard SET procedure is performed by the EW 10, the Merchant server 3 and the Payment Gateway server 5.

- Finally, in step III, after completion of the payment, the Merchant server 3 informs the MA 14 of this fact. The MA 14 passes this message on to the CA 13, which notifies the customer of payment completion.
- 20

- The infrastructure and message flows are a natural extension of any agent-based infrastructure. Implementation may therefore be performed straightforwardly.
- 25

09557383-060101  
TOT090-ES25850



## CLAIMS

1. System for the execution of secure transactions in a multimedia network, comprising a multimedia network with customer stations (2), merchant servers (3), and a payment server (5) connected to it, secure electronic transactions being performed using a secure electronic transactions protocol, comprising the exchange of digital certificates, uniquely identifying the relevant transaction participants and also attesting their privileges at the merchant server, said certificates being managed by a Trusted Third Party Server (9) being connected too to said multimedia network, said payment servers 5 being enabled to validate the digital certificates presented and to process authorisation concerning the payment, said customer stations comprising transactions management means (10), fit for performing said secure electronic transactions protocol and for managing said certificates for the customer station, characterized in a remote customer agent (13), managed by agent parameters received or to be received from said customer station (2) and thus, under the control of said parameters, assisting or representing the customer station in a negotiation process, including selecting products to be presented by the merchant server (3), and payment for selected products in a secure way, under control of said secure electronic transactions protocol and said certificates, being managed by said transactions management means (10).
2. System according to claim 1, characterized in that said customer station (2) comprises an agent interface 12, fit for transmission of codes, parameters and certificates between said customer agent (13) and said transactions management means (10).
3. System according to claim 1, characterized in a remote merchant agent (14), managed by agent parameters received or to be

0957383-060101

received from said merchant station (3) and thus, under the control of said parameters, assisting or representing the merchant station in a negotiation process, including presenting products to the customer agent (13) or the customer station (3), and to have paid for products being selected by the customer agent (13) or the customer station (3), in a secure way, under control of said secure electronic transactions protocol and said certificates.

4. System according to claim 2,

10 characterized in that said negotiation and payment process by said customer agent (13) and said merchant agent (14) is performed within an agent negotiation server (11), connected to said multimedia network (1).

15 5. System according to claim 1,

characterized in that, within said secure electronic transaction protocol, for authentication and authorisation said customer agent (13) transmits a token is encapsulated, comprising an authorisation code for opening  
20 up said transactions management means (10).

6. System according to claim 5,

characterized in that said token is stored within the customer agent (13) in an encrypted form, using a random key, being generated at the customer station (2)  
25 for each new payment process.

7. System according to claim 5,

characterized in that both the customer station (2) and the customer agent (13) comprise a specific communication certificate, payment start messages being  
30 communicated to said transactions management means (10) in encrypted form, using a random session key which, in turn, is sent over in encrypted form, using the customer station's public key related to said communication certificate, said message being signed with the customer  
35 agent's private key related to said communication

00057383.060101

certificate and a time stamp being added to said message in order to prevent replay by malicious parties.

8. Method for the execution of secure transactions in a multimedia network, comprising a multimedia network with
- 5 customer stations (2), merchant servers (3), and a payment server (5) connected to it, secure electronic transactions being performed using a secure electronic transactions protocol, comprising the exchange of digital certificates, uniquely identifying the relevant transaction participants
- 10 and also attesting their privileges at the merchant server, said certificates being managed by a Trusted Third Party Server (9) being connected too to said multimedia network, said payment servers 5 being enabled to validate the digital certificates presented and to process authorisation
- 15 concerning the payment, said customer stations comprising transactions management means (10), fit for performing said secure electronic transactions protocol and for managing said certificates for the customer station, moreover, comprising a remote customer agent (13), managed by agent
- 20 parameters received or to be received from said customer station (2) and thus, under the control of said parameters, assisting or representing the customer station in a negotiation process, including selecting products to be presented by the merchant server (3), and payment for
- 25 selected products in a secure way, under control of said secure electronic transactions protocol and said certificates, being managed by said transactions management means (10), while, moreover, said customer station (2) comprises an agent interface (12), fit for transmission of
- 30 codes, parameters and certificates between said customer agent (13) and said transactions management means (10), and, besides, a remote merchant agent (14), managed by agent parameters received or to be received from said merchant station (3) and thus, under the control of said
- 35 parameters, assisting or representing the merchant station in a negotiation process, including presenting products to

09857383-060101  
TOT990-88825860

the customer agent (13) or the customer station (3), and to have paid for products being selected by the customer agent (13) or the customer station (3), in a secure way, under control of said secure electronic transactions protocol and  
5 said certificates, characterized in the following communication steps:

in a first step, said customer agent (13) requests said merchant agent (14) to pay by credit card, and the merchant agent then informs said merchant server (3) of the  
10 requested payment, while parallel to that the the customer agent (13) initialises said transactions management means (10);

in a second step, a standard secure electronic transaction procedure is performed by the transactions management means  
15 (10), the merchant server (3) and the payment gateway server (5);

in a third, final step, after completion of the payment process, the merchant server (3) informs the merchant agent (14) of that completion of the payment process, and the  
20 merchant agent (14) passes this message on to the customer agent (13), which notifies the customer station (2) of the payment completion.

09057383-060101



```

sequenceDiagram
    participant CA as Cardh. Agent
    participant CH as Card holder
    participant MS as Merchant Server
    participant PG as Payment Gateway
    participant MA as Merchant Agent

    Note over CA, CH, MS, PG, MA: I
    CA->>CH: PayStart
    CH->>MS: Author
    Note over CA, CH, MS, PG, MA: II
    MS->>PG: SET
    Note over CA, CH, MS, PG, MA: III
    PG->>MA: PayInfo
    MA->>PG: PCompl
    PG->>CH: PCompl
    CH->>CA: PCompl
  
```

**FIG. 2**

# PATENT COOPERATION TREATY

From the  
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:

KRUK, Wiggert Johan  
KONINKLIJKE KPN N.V.  
P.O. Box 95321  
NL-2509 CH Den Haag  
PAYS-BAS

## PCT

NOTIFICATION OF TRANSMITTAL OF  
THE INTERNATIONAL PRELIMINARY  
EXAMINATION REPORT  
(PCT Rule 71.1)

Date of mailing (day/month/year)	23.04.2001
-------------------------------------	------------

Applicant's or agent's file reference 402552WO	<b>IMPORTANT NOTIFICATION</b>
---------------------------------------------------	-------------------------------


International application No. PCT/EP99/08157	International filing date (day/month/year) 25/10/1999	Priority date (day/month/year) 02/12/1998
-------------------------------------------------	----------------------------------------------------------	----------------------------------------------

Applicant KONINKLIJKE KPN N.V. et al.
------------------------------------------

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.
2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.
3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.
4. **REMINDER**  
  
The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices) (Article 39(1)) (see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

Name and mailing address of the IPEA/   European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer  Camps i Amigo, M.E.  Tel. +49 89 2399-2237
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------



# PATENT COOPERATION TREATY

## PCT


### INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference <b>402552WO</b>	<b>FOR FURTHER ACTION</b> See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. <b>PCT/EP99/08157</b>	International filing date (day/month/year) <b>25/10/1999</b>	Priority date (day/month/year) <b>02/12/1998</b>
International Patent Classification (IPC) or national classification and IPC <b>G06F17/60</b>		
Applicant <b>KONINKLIJKE KPN N.V. et al.</b>		

- This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
- This REPORT consists of a total of 6 sheets, including this cover sheet.  
  
☐ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).  
  
 These annexes consist of a total of sheets.

- This report contains indications relating to the following items:
  - I ☒ Basis of the report
  - II ☐ Priority
  - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
  - IV ☐ Lack of unity of invention
  - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
  - VI ☐ Certain documents cited
  - VII ☒ Certain defects in the international application
  - VIII ☒ Certain observations on the international application

Date of submission of the demand  <b>08/02/2000</b>	Date of completion of this report  <b>23.04.2001</b>
Name and mailing address of the international preliminary examining authority:   <b>European Patent Office</b> <b>D-80298 Munich</b> <b>Tel. +49 89 2399 - 0 Tx: 523656 epmu d</b> <b>Fax: +49 89 2399 - 4465</b>	Authorized officer  <b>Kruspig, S</b>  Telephone No. <b>+49 89 2399 2536</b>





# INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/EP99/08157

## I. Basis of the report

1. This report has been drawn on the basis of *(substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments (Rules 70.16 and 70.17).)*:

### Description, pages:

1-7 as originally filed

### Claims, No.:

1-8 as originally filed

### Drawings, sheets:

1/2-2/2 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:

**INTERNATIONAL PRELIMINARY  
EXAMINATION REPORT**

International application No. PCT/EP99/08157

☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

*(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)*

6. Additional observations, if necessary:

**V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

**1. Statement**

Novelty (N)	Yes:	Claims	1-8
	No:	Claims	
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-8
Industrial applicability (IA)	Yes:	Claims	1-8
	No:	Claims	

2. Citations and explanations  
**see separate sheet**

**VII. Certain defects in the international application**

The following defects in the form or contents of the international application have been noted:  
**see separate sheet**

**INTERNATIONAL PRELIMINARY  
EXAMINATION REPORT - SEPARATE SHEET**

---

International application No. PCT/EP99/08157

**1. Re Item VIII**

**Certain observations on the international application**

Independent claims 1 and 8 do not meet the requirements of Art. 6 PCT in that the claims are not clear. The claims comprise various possibilities (received or to be received, assisting or representing) which renders the subject-matter put under protection unclear. Furthermore, the parameters received from the customer station are not specified.

**2. Re Item V**

**Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

**2.1. Reference is made to the following documents:**

D1: US-A-5 671 280 (ROSEN SHOLOM S) 23 September 1997 (1997-09-23)

D2: WO 97 26612 A (PERSONAL AGENTS INC) 24 July 1997 (1997-07-24)

**2.2. Claim 1 lacks an inventive step for the following reason:**

D1 discloses an electronic commercial payment system with secure transactions. The system of D1 comprises customer stations (D1, Fig. 6, customer networks 191) and merchant servers (D1, Fig. 6, merchant network 134). Customer and merchant comprise transaction devices (D1, Fig. 4) which include a trusted agent 120. The trusted agent is used to provide secure electronic transactions (D1, Fig. 5A, 5B, 5C, 5D and col. 5, l. 65 to col. 7, l. 22). For this reason it includes (D1, Fig. 5A) a security manager function maintaining eg. trusted agent certificates and an untrusted agent list. Furthermore, cryptographic functions 152 of the trusted agent component make possible secure transactions.

The characterising part of claim 1 is derivable from D1 too. The remote customer agent of claim 1 is comparable to the trusted agent 120 of the transaction device connected to a customer network. In D1 the trusted agent of a customer is managed by parameters received from the customer station. The trusted agent

assists or presents the customer station in a negotiation process. D1 discloses a detailed payment procedure which operates in a secure way. Fig. 14 of D1 illustrates four encryption channels established during a transaction (cf. also D1, col. 12, l. 50 to col. 13, l. 7).

Hence, the characterizing features of claim 1 seem to be quite general in comparison to D1. It follows that a person skilled in secure electronic transactions could derive the subject-matter of claim 1 from D1.

D1 does not disclose a multimedia network. However, from the claim it cannot be seen that a special transaction management is necessary for multimedia.

D2 indicates a document which describes intelligent agents in the sense of a software entity that is capable of performing certain delegated actions on behalf of a user (D2, page 14, last paragraph). Features of the characterising part "customer agent ... representing the customer station in a negotiation process" are derivable for the skilled person from D2 (claim 45).

- 2.3. Method claim 8 is similar to claim 1 in words of a method. The characterizing part of claim 8 indicates 3 communication steps.

The first step is a normal step of a normal payment action by credit card between customer and merchant (eg. remittance advice in Fig. 1 of D1). Customer agent and merchant agent inform (or initialise) transaction management means and merchant server, respectively. D1 also indicates on the customer side and on the merchant side specialised modules (D1, Fig. 6, modules 188, 189, 193, 198) which perform a secure electronic transaction (D1, Fig. 13, step 630).

In D1 the transaction process includes commit routines (D1, col. 18, l. 28-67).

Furthermore, after a successful completion of the payment further modules (trusted agents) get messages to indicate "Payment Successful" (D1, col. 19).

Hence, the final step of claim 8 is derivable from D1 for a person skilled in secure electronic payment.

- 2.4. Dependent system claims 2-7 seem to comprise normal implementation possibilities and thus do not provide features for an allowable claim. The token of claim 5 is comparable to various security information transmissions between customer and merchant in D1. Before the money module payment is performed several signature verification steps are processed (D1, col. 12, lines 3-49).

**INTERNATIONAL PRELIMINARY  
EXAMINATION REPORT - SEPARATE SHEET**

---

International application No. PCT/EP99/08157

**3. Re Item VII**

**Certain defects in the international application**

D1, D2 are not mentioned in the description as the closest prior art documents (Rule 5.1a)ii) PCT).

The applicant's attention is drawn to the fact that, as a consequence of Rule 66.8(a) PCT the examiner is not permitted to carry out any amendments under the PCT procedure, however minor these may be.

# PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

# PCT

NOTIFICATION OF TRANSMITTAL OF  
THE INTERNATIONAL SEARCH REPORT  
OR THE DECLARATION

(PCT Rule 44.1)

To:  
KONINKLIJKE KPN N.V.  
Attn. Klein, Bart  
P.O. Box 95321  
NL-2509 CH Den Haag  
NETHERLANDS

Date of mailing  
(day/month/year) **02/02/2000**

Applicant's or agent's file reference <b>402552W0</b>	<b>FOR FURTHER ACTION</b> See paragraphs 1 and 4 below
----------------------------------------------------------	--------------------------------------------------------

International application No. <b>PCT/EP 99/08157</b>	International filing date (day/month/year) <b>25/10/1999</b>
---------------------------------------------------------	-----------------------------------------------------------------

Applicant  
**KONINKLIJKE KPN N.V. et al.**

1. ☒ The applicant is hereby notified that the International Search Report has been established and is transmitted herewith.

**Filing of amendments and statement under Article 19:**  
The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

**When?** The time limit for filing such amendments is normally 2 months from the date of transmittal of the International Search Report; however, for more details, see the notes on the accompanying sheet.

**Where?** Directly to the International Bureau of WIPO  
34, chemin des Colombettes  
1211 Geneva 20, Switzerland  
Facsimile No.: (41-22) 740.14.35

**For more detailed instructions,** see the notes on the accompanying sheet.

2. ☐ The applicant is hereby notified that no International Search Report will be established and that the declaration under Article 17(2)(a) to that effect is transmitted herewith.

3. ☐ **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Further action(s):** The applicant is reminded of the following:

Shortly after **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90bis.1 and 90bis.3, respectively, before the completion of the technical preparations for international publication.

Within **19 months** from the priority date, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase until 30 months from the priority date (in some Offices even later).

Within **20 months** from the priority date, the applicant must perform the prescribed acts for entry into the national phase before all designated Offices which have not been elected in the demand or in a later election within 19 months from the priority date or could not be elected because they are not bound by Chapter II.

Name and mailing address of the International Searching Authority European Patent Office, P.B. 5818 Patentaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer  <b>Lucia Van Pinxteren</b>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------

## NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the PCT Applicant's Guide, a publication of WIPO.

In these Notes, "Article", "Rule", and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions respectively.

### INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims, description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only.

#### What parts of the International application may be amended?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

#### When?

Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

#### Where not to file the amendments?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

#### How?

Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet must be submitted for each sheet of the claims which, on account of an amendment or amendments, differs from the sheet originally filed.

All the claims appearing on a replacement sheet must be numbered in Arabic numerals. Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively (Administrative Instructions, Section 205(b)).

The amendments must be made in the language in which the international application is to be published.

#### What documents must/may accompany the amendments?

**Letter (Section 205(b)):**

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

## NOTES TO FORM PCT/ISA/220 (continued)

The letter must indicate the differences between the claims as filed and the claims as amended. It must, in particular, indicate, in connection with each claim appearing in the international application (it being understood that identical indications concerning several claims may be grouped), whether

- (i) the claim is unchanged;
- (ii) the claim is cancelled;
- (iii) the claim is new;
- (iv) the claim replaces one or more claims as filed;
- (v) the claim is the result of the division of a claim as filed.

The following examples illustrate the manner in which amendments must be explained in the accompanying letter:

1. [Where originally there were 48 claims and after amendment of some claims there are 51]:  
"Claims 1 to 29, 31, 32, 34, 35, 37 to 48 replaced by amended claims bearing the same numbers; claims 30, 33 and 36 unchanged; new claims 49 to 51 added."
2. [Where originally there were 15 claims and after amendment of all claims there are 11]:  
"Claims 1 to 15 replaced by amended claims 1 to 11."
3. [Where originally there were 14 claims and the amendments consist in cancelling some claims and in adding new claims]:  
"Claims 1 to 6 and 14 unchanged; claims 7 to 13 cancelled; new claims 15, 16 and 17 added." or  
"Claims 7 to 13 cancelled; new claims 15, 16 and 17 added; all other claims unchanged."
4. [Where various kinds of amendments are made]:  
"Claims 1-10 unchanged; claims 11 to 13, 18 and 19 cancelled; claims 14, 15 and 16 replaced by amended claim 14; claim 17 subdivided into amended claims 15, 16 and 17; new claims 20 and 21 added."

### "Statement under article 19(1)" (Rule 46.4)

The amendments may be accompanied by a statement explaining the amendments and indicating any impact that such amendments might have on the description and the drawings (which cannot be amended under Article 19(1)).

The statement will be published with the international application and the amended claims.

**It must be in the language in which the international application is to be published.**

It must be brief, not exceeding 500 words if in English or if translated into English.

It should not be confused with and does not replace the letter indicating the differences between the claims as filed and as amended. It must be filed on a separate sheet and must be identified as such by a heading, preferably by using the words "Statement under Article 19(1)."

It may not contain any disparaging comments on the international search report or the relevance of citations contained in that report. Reference to citations, relevant to a given claim, contained in the international search report may be made only in connection with an amendment of that claim.

### Consequence if a demand for international preliminary examination has already been filed

If, at the time of filing any amendments under Article 19, a demand for international preliminary examination has already been submitted, the applicant must preferably, at the same time of filing the amendments with the International Bureau, also file a copy of such amendments with the International Preliminary Examining Authority (see Rule 62.2(a), first sentence).

### Consequence with regard to translation of the international application for entry into the national phase

The applicant's attention is drawn to the fact that, where upon entry into the national phase, a translation of the claims as amended under Article 19 may have to be furnished to the designated/elected Offices, instead of, or in addition to, the translation of the claims as filed.

For further details on the requirements of each designated/elected Office, see Volume II of the PCT Applicant's Guide.



# PATENT COOPERATION TREATY

# PCT

## INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference <b>402552W0</b>	<b>FOR FURTHER ACTION</b> <small>see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.</small>	
International application No. <b>PCT/EP 99/ 08157</b>	International filing date (day/month/year) <b>25/10/1999</b>	(Earliest) Priority Date (day/month/year) <b>02/12/1998</b>
Applicant  <b>KONINKLIJKE KPN N.V. et al.</b>		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

**1. Basis of the report**

a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

☐ the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. ☐ **Certain claims were found unsearchable** (See Box I).

3. ☐ **Unity of invention is lacking** (see Box II).

4. With regard to the **title**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No.

☒ as suggested by the applicant.

☐ because the applicant failed to suggest a figure.

☐ because this figure better characterizes the invention.

1  
☐ None of the figures.

## INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 99/08157

## A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G06F17/60 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G06F G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 671 280 A (ROSEN SHOLOM S) 23 September 1997 (1997-09-23) column 1, line 1 - line 13 column 2, line 15 - line 50 column 5, line 65 -column 6, line 63 column 9, line 46 -column 10, line 64 --- -/--	1-8



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

## \* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&amp;" document member of the same patent family

Date of the actual completion of the international search

25 January 2000

Date of mailing of the international search report

02/02/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Pedersen, N

## INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 99/08157

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>XUN YI ET AL: "A secure auction-like negotiation protocol for agent-based Internet trading"</p> <p>PROCEEDINGS SEVENTEENTH IEEE SYMPOSIUM ON RELIABLE DISTRIBUTED SYSTEMS (CAT. NO.98CB36281), WEST LAFAYETTE, IN, USA, 20 - 23 October 1998, pages 197-203, XP002100668</p> <p>ISBN 0-8186-9218-9, 1998, Los Alamitos, CA, USA, IEEE Comput. Soc, USA</p> <p>page 197, column 2, line 2 - line 6</p> <p>page 198, column 2, line 5 -page 199, column 2, line 41</p> <p>---</p>	1-8
A	<p>"SET Secure Electronic Transaction Specification, Book 1: Business Description"</p> <p>31 May 1997 (1997-05-31) , SETCO, MASTERCARD INTERNATIONAL, VISA INTERNATIONAL ,</p> <p>(<a href="http://www.setco.org/download.html">HTTP://WWW.SETCO.ORG/DOWNLOAD.HTML</a>)</p> <p>XP002100669</p> <p>Retrieved from the internet 20th April 1999</p> <p>page 30 -page 72</p> <p>---</p>	1-8
A	<p>US 5 790 677 A (SPELMAN JEFFREY F ET AL)</p> <p>4 August 1998 (1998-08-04)</p> <p>column 2, line 6 -column 4, line 39</p> <p>---</p>	1-8
A	<p>WO 97 26612 A (PERSONAL AGENTS INC)</p> <p>24 July 1997 (1997-07-24)</p> <p>page 1, line 11 - line 16</p> <p>page 26, line 20 -page 32, line 19</p> <p>figures 1,2</p> <p>-----</p>	1-8

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 99/08157

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 5671280	A	23-09-1997	AU 699117 B	19-11-1998
			AU 5426496 A	19-03-1997
			CA 2229012 A	06-03-1997
			EP 0886839 A	30-12-1998
			EP 0952562 A	27-10-1999
			HU 9801636 A	28-10-1998
			JP 11500555 T	12-01-1999
			NZ 306096 A	28-10-1998
			PL 325154 A	06-07-1998
			WO 9708665 A	06-03-1997
<hr/>				
US 5790677	A	04-08-1998	NONE	
<hr/>				
WO 9726612	A	24-07-1997	AU 1836297 A	11-08-1997
			CA 2242874 A	24-07-1997
			EP 0876652 A	11-11-1998
<hr/>				

# PATENT COOPERATION TREATY

From the RECEIVING OFFICE

# PCT

To:

Klein, Bart  
KONINKLIJKE KPN N.V.  
P.O. Box 95321  
NL-2509 CH Den Haag  
PAYS-BAS

## NOTIFICATION OF THE INTERNATIONAL APPLICATION NUMBER AND OF THE INTERNATIONAL FILING DATE

(PCT Rule 20.5(c))

Date of mailing  
(day/month/year) **26 -11- 1999**

Applicant's or agent's file reference <b>402552W0</b>		<b>IMPORTANT NOTIFICATION</b>	
International application No. <b>PCT/ EP 99/ 08157</b>	International filing date (day/month/year) <b>25/10/1999</b>	Priority date (day/month/year) <b>02/12/1998</b>	
Applicant <b>KONINKLIJKE KPN N.V.</b>			
Title of the invention			

1. The applicant is hereby notified that the international application has been accorded the international application number and the international filing date indicated above.
2. The applicant is further notified that the record copy of the international application was transmitted to the International Bureau on the above date of mailing.
3. ☐ Other:

\* The International Bureau monitors the transmittal of the record copy by the receiving Office and will notify the applicant (with Form PCT/IB/301) of its receipt. Should the record copy not have been received by the expiration of 14 months from the priority date, the International Bureau will notify the applicant (Rule 22.1(c)).

Name and mailing address of the receiving Office



European Patent Office, P.B. 5818 Patentlaan 2  
NL-2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Maria Peis

*Maria Peis*

# PCT

## REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty.

For receiving Office use only

**PCT/EP 99 / 08157**

International Application No.

**25 OCT 1999 (25.10.99)**  
International Filing Date

**EUROPEAN PATENT OFFICE**  
**PCT INTERNATIONAL APPLICATION**  
Name of receiving Office and "PCT International Application"

Applicant's or agent's file reference  
(if desired) (12 characters maximum) **402552W0**

<b>Box No. I TITLE OF INVENTION</b>	
System for secure transactions	
<b>Box No. II APPLICANT</b>	
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)	
KONINKLIJKE KPN N.V. Stationsplein 7 9726 AE GRONINGEN The Netherlands	
<input type="checkbox"/> This person is also inventor.	
Telephone No. +31 70 3323678	
Facsimile No. +31 70 3323840	
Teleprinter No.	
State (that is, country) of nationality: NL	State (that is, country) of residence: NL
This person is applicant for the purposes of: <input type="checkbox"/> all designated States <input checked="" type="checkbox"/> all designated States except the United States of America <input type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box	
<b>Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)</b>	
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)	
KERKDIJK Hendrikus Oostersingel 23/19 9713 EX GRONINGEN The Netherlands	
This person is: <input type="checkbox"/> applicant only <input checked="" type="checkbox"/> applicant and inventor <input type="checkbox"/> inventor only (If this check-box is marked, do not fill in below.)	
State (that is, country) of nationality: NL	State (that is, country) of residence: NL
This person is applicant for the purposes of: <input type="checkbox"/> all designated States <input type="checkbox"/> all designated States except the United States of America <input checked="" type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box	
<input type="checkbox"/> Further applicants and/or (further) inventors are indicated on a continuation sheet.	
<b>Box No. IV AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE</b>	
The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as: <input checked="" type="checkbox"/> agent <input type="checkbox"/> common representative	
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)	
KLEIN Bart KONINKLIJKE KPN N.V. P.O. BOX 95321 2509 CH THE HAGUE The Netherlands	
Telephone No. +31 70 3323678	
Facsimile No. +31 70 3323840	
Teleprinter No.	
<input type="checkbox"/> Address for correspondence: Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent.	

## Box No.V DESIGNATION OF STATES

The following designations are hereby made under Rule 4.9(a) (mark the applicable check-boxes; at least one must be marked):

## Regional Patent

- ☒ **AP** ARIPO Patent: GH Ghana, GM Gambia, KE Kenya, LS Lesotho, MW Malawi, SD Sudan, SL Sierra Leone, SZ Swaziland, UG Uganda, ZW Zimbabwe, and any other State which is a Contracting State of the Harare Protocol and of the PCT
- ☒ **EA** Eurasian Patent: AM Armenia, AZ Azerbaijan, BY Belarus, KG Kyrgyzstan, KZ Kazakhstan, MD Republic of Moldova, RU Russian Federation, TJ Tajikistan, TM Turkmenistan, and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT
- ☒ **EP** European Patent: AT Austria, BE Belgium, CH and LI Switzerland and Liechtenstein, CY Cyprus, DE Germany, DK Denmark, ES Spain, FI Finland, FR France, GB United Kingdom, GR Greece, IE Ireland, IT Italy, LU Luxembourg, MC Monaco, NL Netherlands, PT Portugal, SE Sweden, and any other State which is a Contracting State of the European Patent Convention and of the PCT
- ☒ **OA** OAPI Patent: BF Burkina Faso, BJ Benin, CF Central African Republic, CG Congo, CI Côte d'Ivoire, CM Cameroon, GA Gabon, GN Guinea, GW Guinea-Bissau, ML Mali, MR Mauritania, NE Niger, SN Senegal, TD Chad, TG Togo, and any other State which is a member State of OAPI and a Contracting State of the PCT (if other kind of protection or treatment desired, specify on dotted line)

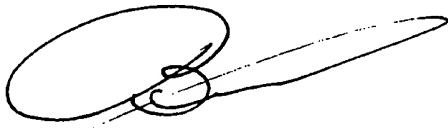
## National Patent (if other kind of protection or treatment desired, specify on dotted line):

- |                                                                                     |                                                                                         |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> <b>AE</b> United Arab Emirates                  | <input checked="" type="checkbox"/> <b>LR</b> Liberia                                   |
| <input checked="" type="checkbox"/> <b>AL</b> Albania                               | <input checked="" type="checkbox"/> <b>LS</b> Lesotho                                   |
| <input checked="" type="checkbox"/> <b>AM</b> Armenia                               | <input checked="" type="checkbox"/> <b>LT</b> Lithuania                                 |
| <input checked="" type="checkbox"/> <b>AT</b> Austria                               | <input checked="" type="checkbox"/> <b>LU</b> Luxembourg                                |
| <input checked="" type="checkbox"/> <b>AU</b> Australia                             | <input checked="" type="checkbox"/> <b>LV</b> Latvia                                    |
| <input checked="" type="checkbox"/> <b>AZ</b> Azerbaijan                            | <input checked="" type="checkbox"/> <b>MD</b> Republic of Moldova                       |
| <input checked="" type="checkbox"/> <b>BA</b> Bosnia and Herzegovina                | <input checked="" type="checkbox"/> <b>MG</b> Madagascar                                |
| <input checked="" type="checkbox"/> <b>BB</b> Barbados                              | <input checked="" type="checkbox"/> <b>MK</b> The former Yugoslav Republic of Macedonia |
| <input checked="" type="checkbox"/> <b>BG</b> Bulgaria                              |                                                                                         |
| <input checked="" type="checkbox"/> <b>BR</b> Brazil                                | <input checked="" type="checkbox"/> <b>MN</b> Mongolia                                  |
| <input checked="" type="checkbox"/> <b>BY</b> Belarus                               | <input checked="" type="checkbox"/> <b>MW</b> Malawi                                    |
| <input checked="" type="checkbox"/> <b>CA</b> Canada                                | <input checked="" type="checkbox"/> <b>MX</b> Mexico                                    |
| <input checked="" type="checkbox"/> <b>CH and LI</b> Switzerland and Liechtenstein  | <input checked="" type="checkbox"/> <b>NO</b> Norway                                    |
| <input checked="" type="checkbox"/> <b>CN</b> China                                 | <input checked="" type="checkbox"/> <b>NZ</b> New Zealand                               |
| <input checked="" type="checkbox"/> <b>CU</b> Cuba                                  | <input checked="" type="checkbox"/> <b>PL</b> Poland                                    |
| <input checked="" type="checkbox"/> <b>CZ</b> Czech Republic                        | <input checked="" type="checkbox"/> <b>PT</b> Portugal                                  |
| <input checked="" type="checkbox"/> <b>DE</b> Germany                               | <input checked="" type="checkbox"/> <b>RO</b> Romania                                   |
| <input checked="" type="checkbox"/> <b>DK</b> Denmark                               | <input checked="" type="checkbox"/> <b>RU</b> Russian Federation                        |
| <input checked="" type="checkbox"/> <b>EE</b> Estonia                               | <input checked="" type="checkbox"/> <b>SD</b> Sudan                                     |
| <input checked="" type="checkbox"/> <b>ES</b> Spain                                 | <input checked="" type="checkbox"/> <b>SE</b> Sweden                                    |
| <input checked="" type="checkbox"/> <b>FI</b> Finland                               | <input checked="" type="checkbox"/> <b>SG</b> Singapore                                 |
| <input checked="" type="checkbox"/> <b>GB</b> United Kingdom                        | <input checked="" type="checkbox"/> <b>SI</b> Slovenia                                  |
| <input checked="" type="checkbox"/> <b>GD</b> Grenada                               | <input checked="" type="checkbox"/> <b>SK</b> Slovakia                                  |
| <input checked="" type="checkbox"/> <b>GE</b> Georgia                               | <input checked="" type="checkbox"/> <b>SL</b> Sierra Leone                              |
| <input checked="" type="checkbox"/> <b>GH</b> Ghana                                 | <input checked="" type="checkbox"/> <b>TJ</b> Tajikistan                                |
| <input checked="" type="checkbox"/> <b>GM</b> Gambia                                | <input checked="" type="checkbox"/> <b>TM</b> Turkmenistan                              |
| <input checked="" type="checkbox"/> <b>HR</b> Croatia                               | <input checked="" type="checkbox"/> <b>TR</b> Turkey                                    |
| <input checked="" type="checkbox"/> <b>HU</b> Hungary                               | <input checked="" type="checkbox"/> <b>TT</b> Trinidad and Tobago                       |
| <input checked="" type="checkbox"/> <b>ID</b> Indonesia                             | <input checked="" type="checkbox"/> <b>UA</b> Ukraine                                   |
| <input checked="" type="checkbox"/> <b>IL</b> Israel                                | <input checked="" type="checkbox"/> <b>UG</b> Uganda                                    |
| <input checked="" type="checkbox"/> <b>IN</b> India                                 | <input checked="" type="checkbox"/> <b>US</b> United States of America                  |
| <input checked="" type="checkbox"/> <b>IS</b> Iceland                               |                                                                                         |
| <input checked="" type="checkbox"/> <b>JP</b> Japan                                 | <input checked="" type="checkbox"/> <b>UZ</b> Uzbekistan                                |
| <input checked="" type="checkbox"/> <b>KE</b> Kenya                                 | <input checked="" type="checkbox"/> <b>VN</b> Viet Nam                                  |
| <input checked="" type="checkbox"/> <b>KG</b> Kyrgyzstan                            | <input checked="" type="checkbox"/> <b>YU</b> Yugoslavia                                |
| <input checked="" type="checkbox"/> <b>KP</b> Democratic People's Republic of Korea | <input checked="" type="checkbox"/> <b>ZA</b> South Africa                              |
|                                                                                     | <input checked="" type="checkbox"/> <b>ZW</b> Zimbabwe                                  |
| <input checked="" type="checkbox"/> <b>KR</b> Republic of Korea                     |                                                                                         |
| <input checked="" type="checkbox"/> <b>KZ</b> Kazakhstan                            |                                                                                         |
| <input checked="" type="checkbox"/> <b>LC</b> Saint Lucia                           |                                                                                         |
| <input checked="" type="checkbox"/> <b>LK</b> Sri Lanka                             |                                                                                         |

Check-boxes reserved for designating States which have become party to the PCT after issuance of this sheet:

- ☐ .....  
☐ .....

**Precautionary Designation Statement:** In addition to the designations made above, the applicant also makes under Rule 4.9(b) all other designations which would be permitted under the PCT except any designation(s) indicated in the Supplemental Box as being excluded from the scope of this statement. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit. (Confirmation of a designation consists of the filing of a notice specifying that designation and the payment of the designation and confirmation fees. Confirmation must reach the receiving Office within the 15-month time limit.)

<b>Box No. VI PRIORITY CLAIM</b>					<input type="checkbox"/> Further priority claims are indicated in the Supplemental Box.
Filing date of earlier application (day/month/year)	Number of earlier application	Where earlier application is:			
		national application: country	regional application: regional Office	international application: receiving Office	
item (1) (2 DEC 1998) 02.12.1998	98204063.6	[EP]	A EP		
item (2)					
item (3)					
<input checked="" type="checkbox"/> The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) (only if the earlier application was filed with the Office which for the purposes of the present international application is the receiving Office) identified above as item(s): EP 98204063.6					
<small>* Where the earlier application is an ARIPO application, it is mandatory to indicate in the Supplemental Box at least one country party to the Paris Convention for the Protection of Industrial Property for which that earlier application was filed (Rule 4.10(b)(ii)). See Supplemental Box.</small>					
<b>Box No. VII INTERNATIONAL SEARCHING AUTHORITY</b>					
<b>Choice of International Searching Authority (ISA)</b> <small>(if two or more International Searching Authorities are competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used):</small>		<b>Request to use results of earlier search; reference to that search</b> (if an earlier search has been carried out by or requested from the International Searching Authority):			
ISA / EP		Date (day/month/year)	Number	Country (or regional Office)	
		21 APRIL 1999		EP	
<b>Box No. VIII CHECK LIST: LANGUAGE OF FILING</b>					
This international application contains the following number of sheets: request : 4 description (excluding sequence listing part) : 7 claims : 4 abstract : 1 drawings : 2 sequence listing part of description : Total number of sheets : 18		This international application is accompanied by the item(s) marked below: 1. <input checked="" type="checkbox"/> fee calculation sheet 2. <input checked="" type="checkbox"/> separate signed power of attorney 3. <input checked="" type="checkbox"/> copy of general power of attorney; reference number, if any: 4. <input type="checkbox"/> statement explaining lack of signature 5. <input checked="" type="checkbox"/> priority document(s) identified in Box No. VI as item(s): 6. <input type="checkbox"/> translation of international application into (language): 7. <input type="checkbox"/> separate indications concerning deposited microorganism or other biological material 8. <input type="checkbox"/> nucleotide and/or amino acid sequence listing in computer readable form 9. <input checked="" type="checkbox"/> other (specify): search report			
Figure of the drawings which should accompany the abstract: 1		Language of filing of the international application: English			
<b>Box No. IX SIGNATURE OF APPLICANT OR AGENT</b>					
Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request).					
 KLEIN Bart					

For receiving Office use only		2. Drawings: <input checked="" type="checkbox"/> received: 20/EP <input type="checkbox"/> not received:
1. Date of actual receipt of the purported international application:	25 OCT 1999 (25.10.99)	
3. Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application:		
4. Date of timely receipt of the required corrections under PCT Article 11(2):		
5. International Searching Authority (if two or more are competent): ISA /	6. <input type="checkbox"/> Transmittal of search copy delayed until search fee is paid.	

For International Bureau use only
Date of receipt of the record copy by the International Bureau:



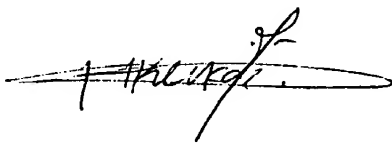
**Supplemental Box** *If the Supplemental Box is not used, this sheet should not be included in the request.*

1. If, in any of the Boxes, the space is insufficient to furnish all the information: in such case, write "Continuation of Box No. ..." [indicate the number of the Box] and furnish the information in the same manner as required according to the captions of the Box in which the space was insufficient, in particular:

- (i) if more than two persons are involved as applicants and/or inventors and no "continuation sheet" is available: in such case, write "Continuation of Box No. III" and indicate for each additional person the same type of information as required in Box No. III. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below;
- (ii) if, in Box No. II or in any of the sub-boxes of Box No. III, the indication "the States indicated in the Supplemental Box" is checked: in such case, write "Continuation of Box No. II" or "Continuation of Box No. III" or "Continuation of Boxes No. II and No. III" (as the case may be), indicate the name of the applicant(s) involved and, next to (each) such name, the State(s) (and/or, where applicable, ARIPO, Eurasian, European or OAPI patent) for the purposes of which the named person is applicant;
- (iii) if, in Box No. II or in any of the sub-boxes of Box No. III, the inventor or the inventor/applicant is not inventor for the purposes of all designated States or for the purposes of the United States of America: in such case, write "Continuation of Box No. II" or "Continuation of Box No. III" or "Continuation of Boxes No. II and No. III" (as the case may be), indicate the name of the inventor(s) and, next to (each) such name, the State(s) (and/or, where applicable, ARIPO, Eurasian, European or OAPI patent) for the purposes of which the named person is inventor;
- (iv) if, in addition to the agent(s) indicated in Box No. IV, there are further agents: in such case, write "Continuation of Box No. IV" and indicate for each further agent the same type of information as required in Box No. IV;
- (v) if, in Box No. V, the name of any State (or OAPI) is accompanied by the indication "patent of addition," or "certificate of addition," or if, in Box No. V, the name of the United States of America is accompanied by an indication "continuation" or "continuation-in-part": in such case, write "Continuation of Box No. V" and the name of each State involved (or OAPI), and after the name of each such State (or OAPI), the number of the parent title or parent application and the date of grant of the parent title or filing of the parent application;
- (vi) if, in Box No. VI, there are more than three earlier applications whose priority is claimed: in such case, write "Continuation of Box No. VI" and indicate for each additional earlier application the same type of information as required in Box No. VI;
- (vii) if, in Box No. VI, the earlier application is an ARIPO application: in such case, write "Continuation of Box No. VI", specify the number of the item corresponding to that earlier application and indicate at least one country party to the Paris Convention for the Protection of Industrial Property for which that earlier application was filed.

2. If, with regard to the precautionary designation statement contained in Box No. V, the applicant wishes to exclude any State(s) from the scope of that statement: in such case, write "Designation(s) excluded from precautionary designation statement" and indicate the name or two-letter code of each State so excluded.

3. If the applicant claims, in respect of any designated Office, the benefits of provisions of the national law concerning non-prejudicial disclosures or exceptions to lack of novelty: in such case, write "Statement concerning non-prejudicial disclosures or exceptions to lack of novelty" and furnish that statement below.



KERKDIJK  
Hendrikus

# PATENT COOPERATION TREATY

From the  
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

# PCT

To:

KRUK, Wiggert Johan  
KONINKLIJKE KPN N.V.  
P.O. Box 95321  
NL-2509 CH Den Haag  
PAYS-BAS

## NOTIFICATION OF RECEIPT OF DEMAND BY COMPETENT INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

(PCT Rules 59.3(e) and 61.1(b), first sentence  
and Administrative Instructions, Section 601(a))

Date of mailing  
(day/month/year)

02. 03. 00

Applicant's or agent's file reference

402552W0

### IMPORTANT NOTIFICATION

International application No.

PCT/ EP 99/ 08157

International filing date (day/month/year)

25/10/1999

Priority date (day/month/year)

02/12/1998

Applicant

KONINKLIJKE KPN N.V. et al.

1. The applicant is hereby notified that this International Preliminary Examining Authority considers the following date as the date of receipt of the demand for international preliminary examination of the international application:

08/02/2000

2. This date of receipt is:



the actual date of receipt of the demand by this Authority (Rule 61.1(b)).



the actual date of receipt of the demand on behalf of this Authority (Rule 59.3(e)).



the date on which this Authority has, in response to the invitation to correct defects in the demand (Form PCT/IPEA/404), received the required corrections.

3. ☐ **ATTENTION:** That date of receipt is **AFTER** the expiration of 19 months from the priority date. Consequently, the election(s) made in the demand does (do) not have the effect of postponing the entry into the national phase until 30 months from the priority date (or later in some Offices) (Article 39(1)). Therefore, the acts for entry into the national phase must be performed within 20 months from the priority date (or later in some Offices) (Article 22). For details, see the *PCT Applicant's Guide*, Volume II.



(If applicable) This notification confirms the information given by telephone, facsimile transmission or in person on:

4. Only where paragraph 3 applies, a copy of this notification has been sent to the International Bureau.

Name and mailing address of the IPEA/



European Patent Office  
D-80298 Munich  
Tel. (+49-89) 2399-0, Tx: 523656 epmu d  
Fax: (+49-89) 2399-4465

Authorized officer

MOSER A R

Tel. (+49-89) 2399-8240



The demand must be filed directly with the competent International Preliminary Examining Authority or, if two or more Authorities are competent, with the one chosen by the applicant. The full name or two-letter code of that Authority may be indicated by the applicant on the line below:

IPEA/ EP

# PCT

## CHAPTER II

### DEMAND

under Article 31 of the Patent Cooperation Treaty:  
The undersigned requests that the international application specified below be the subject of international preliminary examination according to the Patent Cooperation Treaty and hereby elects all eligible States (except where otherwise indicated).

For International Preliminary Examining Authority use only	
Identification of IPEA	Date of receipt of DEMAND
<b>Box No. I IDENTIFICATION OF THE INTERNATIONAL APPLICATION</b>	
International application No. PCT/EP99/08157	International filing date (day/month/year) (25/10/99) 25 October 1999
Applicant's or agent's file reference (Earliest) Priority date (day/month/year) (02/12/98) 02 December 1998	
Title of invention System for secure transactions.	
<b>Box No. II APPLICANT(S)</b>	
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)  KONINKLIJKE KPN N.V. 7 Stationsplein 9726 AE GRONINGEN The Netherlands	
Telephone No.: +31 70 332 36 78 Facsimile No.: +31 70 332 38 40 Teleprinter No.:	
State (that is, country) of nationality: NL	State (that is, country) of residence: NL
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)  KERKDIJK, Hendrikus Oostersingel 23/19 9713 EX GRONINGEN The Netherlands	
State (that is, country) of nationality: NL	State (that is, country) of residence: NL
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)  	
State (that is, country) of nationality:	State (that is, country) of residence:
<input type="checkbox"/> Further applicants are indicated on a continuation sheet.	

**Box No. III AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE**The following person is ☒ agent ☐ common representativeand ☒ has been appointed earlier and represents the applicant(s) also for international preliminary examination.☐ is hereby appointed and any earlier appointment of (an) agent(s)/common representative is hereby revoked.☐ is hereby appointed, specifically for the procedure before the International Preliminary Examining Authority, in addition to the agent(s)/common representative appointed earlier.Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

KRUK, Wiggert Johan  
 KONINKLIJKE KPN N.V.  
 P.O. BOX 95321  
 2509 CH The Hague  
 The Netherlands

Telephone No.:

+31 70 332 36 78

Facsimile No.:

+31 70 332 38 40

Teleprinter No.:

☐ Address for correspondence: Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent.**Box No. IV BASIS FOR INTERNATIONAL PRELIMINARY EXAMINATION****Statement concerning amendments:\***

1. The applicant wishes the international preliminary examination to start on the basis of:

☒ the international application as originally filedthe description ☒ as originally filed☐ as amended under Article 34the claims ☒ as originally filed☐ as amended under Article 19 (together with any accompanying statement)☐ as amended under Article 34the drawings ☒ as originally filed☐ as amended under Article 342. ☐ The applicant wishes any amendment to the claims under Article 19 to be considered as reversed.3. ☐ The applicant wishes the start of the international preliminary examination to be postponed until the expiration of 20 months from the priority date unless the International Preliminary Examining Authority receives a copy of any amendments made under Article 19 or a notice from the applicant that he does not wish to make such amendments (Rule 69.1(d)). *(This check-box may be marked only where the time limit under Article 19 has not yet expired.)*

\* Where no check-box is marked, international preliminary examination will start on the basis of the international application as originally filed or, where a copy of amendments to the claims under Article 19 and/or amendments of the international application under Article 34 are received by the International Preliminary Examining Authority before it has begun to draw up a written opinion or the international preliminary examination report, as so amended.

Language for the purposes of international preliminary examination: English☒ which is the language in which the international application was filed.☐ which is the language of a translation furnished for the purposes of international search.☐ which is the language of publication of the international application.☐ which is the language of the translation (to be) furnished for the purposes of international preliminary examination.**Box No. V ELECTION OF STATES**The applicant hereby elects all eligible States *(that is, all States which have been designated and which are bound by Chapter II of the PCT)*

excluding the following States which the applicant wishes not to elect:

**Box No. VI CHECK LIST**

The demand is accompanied by the following elements, in the language referred to in Box No. IV, for the purposes of international preliminary examination:

- |                                                                          |   |        |
|--------------------------------------------------------------------------|---|--------|
| 1. translation of international application                              | : | sheets |
| 2. amendments under Article 34                                           | : | sheets |
| 3. copy (or, where required, translation) of amendments under Article 19 | : | sheets |
| 4. copy (or, where required, translation) of statement under Article 19  | : | sheets |
| 5. letter                                                                | : | sheets |
| 6. other (specify)                                                       | : | sheets |

For International Preliminary Examining Authority use only

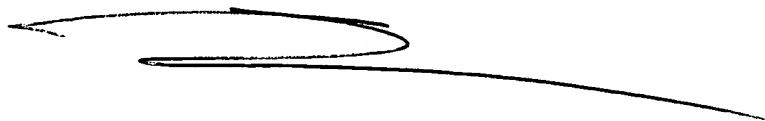
received	not received
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

The demand is also accompanied by the item(s) marked below:

- |                                                                                                     |                                                                                                     |
|-----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| 1. <input checked="" type="checkbox"/> fee calculation sheet                                        | 4. <input type="checkbox"/> statement explaining lack of signature                                  |
| 2. <input type="checkbox"/> separate signed power of attorney                                       | 5. <input type="checkbox"/> nucleotide and or amino acid sequence listing in computer readable form |
| 3. <input checked="" type="checkbox"/> copy of general power of attorney; reference number, if any: | 6. <input type="checkbox"/> other (specify):                                                        |

**Box No. VII SIGNATURE OF APPLICANT, AGENT OR COMMON REPRESENTATIVE**

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the demand).



Wiggert Johan Kruk

For International Preliminary Examining Authority use only

- Date of actual receipt of DEMAND:
- Adjusted date of receipt of demand due to CORRECTIONS under Rule 60.1(b):
- ☐ The date of receipt of the demand is AFTER the expiration of 19 months from the priority date and item 4 or 5, below, does not apply.
 ☐ The applicant has been informed accordingly.
- ☐ The date of receipt of the demand is WITHIN the period of 19 months from the priority date as extended by virtue of Rule 80.5.
- ☐ Although the date of receipt of the demand is after the expiration of 19 months from the priority date, the delay in arrival is EXCUSED pursuant to Rule 82.

For International Bureau use only

Demand received from IPEA on:

## PCT

## FEE CALCULATION SHEET

Annex to the Demand for international preliminary examination

International application No. <u>PCT/EP99/08157</u> Applicant's or agent's file reference <u>402552W0</u>	For International Preliminary Examining Authority use only Date stamp of the IPEA
Applicant <p style="text-align: center;">KONINKLIJKE KPN N.V.</p>	
Calculation of prescribed fees  1. Preliminary examination fee ..... <span style="border: 1px solid black; padding: 2px;">EUR 1533</span> <span style="border: 1px solid black; padding: 2px; float: right;">P</span>  2. Handling fee <i>(Applicants from certain States are entitled to a reduction of 75% of the handling fee. Where the applicant is (or all applicants are) so entitled, the amount to be entered at H is 25% of the handling fee.)</i> ..... <span style="border: 1px solid black; padding: 2px;">EUR 147</span> <span style="border: 1px solid black; padding: 2px; float: right;">H</span>  3. Total of prescribed fees Add the amounts entered at P and H and enter total in the TOTAL box ..... <span style="border: 1px solid black; padding: 2px; display: inline-block; width: 150px;">EUR 1680</span> <div style="border: 1px solid black; width: 100px; margin-left: auto; text-align: center;">TOTAL</div>	
Mode of Payment  <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <input checked="" type="checkbox"/> authorization to charge deposit account with the IPEA (see below)  <input type="checkbox"/> cheque  <input type="checkbox"/> postal money order  <input type="checkbox"/> bank draft         </div> <div style="width: 45%;"> <input type="checkbox"/> cash  <input type="checkbox"/> revenue stamps  <input type="checkbox"/> coupons  <input type="checkbox"/> other (specify):         </div> </div>	
Deposit Account Authorization <i>(this mode of payment may not be available at all IPEAs)</i>  The IPEA/ <u>EP</u> <input checked="" type="checkbox"/> is hereby authorized to charge the total fees indicated above to my deposit account.  <input checked="" type="checkbox"/> <i>(this check-box may be marked only if the conditions for deposit accounts of the IPEA so permit)</i> is hereby authorized to charge any deficiency or credit any overpayment in the total fees indicated above to my deposit account.	
<u>28090011</u> Deposit Account Number	<u>7 February 2000</u> Date (day/month/year)
<div style="text-align: right;">           Signature <u>Wiggert Johan Kruk</u> </div>	

1 **ALLGEMEINE VOLLMACHT  
GENERAL AUTHORISATION  
POUVOIR GENERAL**

Nur für amtlichen Gebrauch / For official use only  
Cadre réservé à l'administration  
Nr. der allgemeinen Vollmacht / General Authorisation No.  
N° du pouvoir général

21396 (rev.)

2 Ich (Wir) / I (We) / Je (Nous)

Koninklijke KPN N.V.

Stationsplein 7

9726 AE GRONINGEN

The Netherlands

3 bevollmächtigte(n) hiermit / do hereby authorise / autorise (autorisons) par la présente

KLEIN, Bart (Professional Representative)

KRUK, Wiggert Johan (Professional Representative)

mailing address: Koninklijke KPN N.V.  
Intellectual Property Group  
P.O. Box 95321  
2509 CH THE HAGUE  
The Netherlands

4 mich (uns) in den durch das Europäische Patentübereinkommen geschaffenen Verfahren in allen meinen (unseren) Patentangelegenheiten zu vertreten, alle Handlungen für mich (uns) vorzunehmen und Zahlungen für mich (uns) in Empfang zu nehmen.  
to represent me (us) in all proceedings established by the European Patent Convention and to act for me (us) in all patent transactions and to receive payments on my (our) behalf.

à me (nous) représenter pour ce qui concerne toutes mes (nos) affaires de brevet dans toute procédure instituée par la Convention sur le brevet européen et, à ce titre, à agir en mon (notre) nom et à recevoir des paiements pour mon (notre) compte.

☒ Die Vollmacht gilt auch für Verfahren nach dem Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens.  
This authorisation shall also apply to the same extent to any proceedings established by the Patent Cooperation Treaty.  
Ce pouvoir s'applique également à toute procédure instituée par le Traité de coopération en matière de brevets.

☐ Weitere Vertreter sind auf einem gesonderten Blatt angegeben. / Additional representatives indicated on supplementary sheet.  
Les autres mandataires sont mentionnés sur une feuille supplémentaire.

5 ☒ Untervollmacht kann erteilt werden. / Sub-authorisation may be given. / Le pouvoir pourra être délégué.

6 ☒ Bitte die gelbe Kopie, ergänzt um die Nr. der allgemeinen Vollmacht, an den Vollmachtgeber zurücksenden.  
Please return the yellow copy, supplemented by the General Authorisation No., to the authorisor.  
Prière de renvoyer la copie jaune au mandant, munie du n° du pouvoir général.

Ort/Place/Lieu The Hague

Datum/Date April 27, 1999

Unterschrift(en) / Signature(s)



KLEIN, Bart (Professional Representative)

7 Das Formblatt muß vom (von den) Vollmachtgeber(n) (bei juristischen Personen vom Unterschriftsberechtigten) eigenhändig unterzeichnet sein. Nach der Unterschrift bitte den (die) Namen des (der) Unterzeichneten mit Schreibmaschine wiederholen (bei juristischen Personen die Stellung des Unterschriftsberechtigten innerhalb der Gesellschaft angeben).

The form must bear the personal signature(s) of the authorisor(s) (in the case of legal persons, that of the officer empowered to sign). After the signature, please type the name(s) of the signatory(ies) adding, in the case of legal persons, his (their) position within the company.

Le formulaire doit être signé de la propre main du (des) mandant(s) (dans le cas de personnes morales, de la personne ayant qualité pour signer). Veuillez ajouter à la machine, après la signature, le (les) nom(s) du (des) signataire(s) en mentionnant, dans le cas de personnes morales, ses (leurs) fonctions au sein de la société.

M.H

## PATENT COOPERATION TREATY

## PCT

## INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 402552W0	<b>FOR FURTHER ACTION</b> see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
International application No. PCT/EP 99/ 08157	International filing date (day/month/year) 25/10/1999	(Earliest) Priority Date (day/month/year) 02/12/1998
Applicant  KONINKLIJKE KPN N.V. et al.		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.



It is also accompanied by a copy of each prior art document cited in this report.

**1. Basis of the report**

- a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.



the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

- b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :



contained in the international application in written form.



filed together with the international application in computer readable form.



furnished subsequently to this Authority in written form.



furnished subsequently to this Authority in computer readable form.



the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.



the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. ☐ **Certain claims were found unsearchable** (See Box I).

3. ☐ **Unity of invention is lacking** (see Box II).

**4. With regard to the title,**

the text is approved as submitted by the applicant.



the text has been established by this Authority to read as follows:

**5. With regard to the abstract,**

the text is approved as submitted by the applicant.



the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

**6. The figure of the drawings to be published with the abstract is Figure No.**

as suggested by the applicant.



because the applicant failed to suggest a figure.



because this figure better characterizes the invention.

1

None of the figures.



# INTERNATIONAL SEARCH REPORT

International Application No.  
PCT/EP 99/08157

**A. CLASSIFICATION OF SUBJECT MATTER**  
IPC 7 G06F17/60 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
IPC 7 G06F G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 671 280 A (ROSEN SHOLOM S) 23 September 1997 (1997-09-23) column 1, line 1 - line 13 column 2, line 15 - line 50 column 5, line 65 - column 6, line 63 column 9, line 46 - column 10, line 64 --- -/--	1-8



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"Z" document member of the same patent family

Date of the actual completion of the international search

25 January 2000

Date of mailing of the international search report

02/02/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Pedersen, N

# INTERNATIONAL SEARCH REPORT

International Application No  
PCT/EP 99/08157

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>XUN YI ET AL: "A secure auction-like negotiation protocol for agent-based Internet trading"</p> <p>PROCEEDINGS SEVENTEENTH IEEE SYMPOSIUM ON RELIABLE DISTRIBUTED SYSTEMS (CAT. NO.98CB36281), WEST LAFAYETTE, IN, USA, 20 - 23 October 1998, pages 197-203, XP002100668</p> <p>ISBN 0-8186-9218-9, 1998, Los Alamitos, CA, USA, IEEE Comput. Soc, USA</p> <p>page 197, column 2, line 2 - line 6</p> <p>page 198, column 2, line 5 -page 199, column 2, line 41</p> <p>---</p>	1-8
A	<p>"SET Secure Electronic Transaction Specification, Book 1: Business Description"</p> <p>31 May 1997 (1997-05-31) , SETCO, MASTERCARD INTERNATIONAL, VISA INTERNATIONAL ,</p> <p>(HTTP://WWW.SETCO.ORG/DOWNLOAD.HTML)</p> <p>XP002100669</p> <p>Retrieved from the internet 20th April 1999</p> <p>page 30 -page 72</p> <p>---</p>	1-8
A	<p>US 5 790 677 A (SPELMAN JEFFREY F ET AL)</p> <p>4 August 1998 (1998-08-04)</p> <p>column 2, line 6 -column 4, line 39</p> <p>---</p>	1-8
A	<p>WO 97 26612 A (PERSONAL AGENTS INC)</p> <p>24 July 1997 (1997-07-24)</p> <p>page 1, line 11 - line 16</p> <p>page 26, line 20 -page 32, line 19</p> <p>figures 1,2</p> <p>-----</p>	1-8

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 99/08157

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5671280 A	23-09-1997	AU 699117 B AU 5426496 A CA 2229012 A EP 0886839 A EP 0952562 A HU 9801636 A JP 11500555 T NZ 306096 A PL 325154 A WO 9708665 A	19-11-1998 19-03-1997 06-03-1997 30-12-1998 27-10-1999 28-10-1998 12-01-1999 28-10-1998 06-07-1998 06-03-1997
US 5790677 A	04-08-1998	NONE	
WO 9726612 A	24-07-1997	AU 1836297 A CA 2242874 A EP 0876652 A	11-08-1997 24-07-1997 11-11-1998